

Łódź, dnia 18.11.2025 r.

ZAPYTANIE OFERTOWE

Wartość zamówienia nie przekracza kwoty 130 000,00 zł netto.

Zamawiający, Muzeum Sztuki w Łodzi zaprasza do złożenia ofert na **Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi. AG.271.10.2025.ZO**

I. ZAMAWIAJACY:

Muzeum Sztuki w Łodzi, 90-734 Łódź ul. Więckowskiego 36

Regon: 000 277 500 NIP: 724 10 00 146

E-mail: muzeum@msl.org.pl

www.msl.org.pl

Osoba do kontaktu:

Aleksandra Schiewe

II. OPIS PRZEDMIOTU ZAMÓWIENIA:

1. Przedmiotem zamówienia jest **Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi. Zakup urządzenia firewall typu premium (wraz z wdrożeniem oraz licencjami)**. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 3 do zapytania (OPZ).
2. Przedmiot zamówienia musi być fabrycznie nowy i nieużywany, pochodzić z produkcji nie wcześniej niż z 2025 roku, posiadać stosowne i aktualnie obowiązujące certyfikaty, atesty, raporty dopuszczające wyposażenia do sprzedaży i użytkowania na terenie RP. Wykonawca jest zobowiązany zapewnić bezpłatny serwis gwarancyjny wyposażenia w okresie udzielonej gwarancji.
3. Zamawiający dopuszcza rozwiązania równoważne pod warunkiem spełnienia tego samego poziomu technologicznego, wydajnościowego i funkcjonalnego założonego w Opisie przedmiotu zamówienia. Wszystkie ewentualne nazwy własne i marki handlowe systemów, urządzeń i wyposażenie zawarte w OPZ, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego. Poprzez pojęcie urządzeń równoważnych należy rozumieć poprzez zapewniające uzyskanie parametrów technicznych nie gorszych od założonych OPZ.
4. Równoważne produkty i urządzenia muszą być dopuszczone do obrotu i stosowania zgodnie z obowiązującym prawem. Wykonawca, który powołuje się na rozwiązania równoważne opisane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego produkty i urządzenia spełniają wymagania określone przez Zamawiającego. Obowiązek Wykonawcy wykazania równoważności produktu spoczywa na Wykonawcy.
5. Termin płatności do 30 dni.
6. Wykonawca zapewni 36 miesięczny okres gwarancji.
7. W celu potwierdzenia, że oferowane dostawy spełniają określone przez Zamawiającego wymagania, Wykonawca zobowiązany jest złożyć wraz z ofertą specyfikację techniczną producenta zaoferowanego modelu (np. opisy

techniczne, karty katalogowe, prospekty, ulotki, instrukcje użytkowania, fotografie) dotyczącą parametrów każdego oferowanego towaru, zawierającą: nazwę towaru, nazwę producenta oraz opis parametrów technicznych potwierdzających zgodność z wymaganiami określonymi w Załączniku nr 3 do zapytania – Opis Przedmiotu Zamówienia.

8. Jeżeli dokumenty, o których mowa w pkt. 5 powyżej, nie będą potwierdzały wszystkich wymaganych parametrów, Wykonawca zobowiązany jest je wskazać i złożyć oświadczenie, że oferowany towar spełnia wszystkie wymagane parametry techniczne.
9. Każdy z dokumentów, o których mowa w pkt. 5 powyżej, musi być przyporządkowany do danego sprzętu poprzez podanie nazwy oraz numeru pozycji z tabeli stanowiącej załącznik nr 1 do zapytania, co ma na celu zapewnienie jednoznacznej identyfikacji zaoferowanego modelu.
10. Jeżeli Wykonawca nie złoży dokumentów, o których mowa w pkt. 5 powyżej lub będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
11. Jeżeli któryś z dokumentów, o których mowa w pkt. 5 powyżej, sporządzony jest w języku obcym, dokument taki należy złożyć wraz z tłumaczeniem na język polski.
12. Zamawiający nie przewiduje udzielania zaliczek na poczet wykonania zamówienia.
13. Zamawiający nie dopuszcza składania ofert częściowych i wariantowych.
14. Planowany termin podpisania umowy: listopad 2025 r.

III. TERMIN I MIEJSCE REALIZACJI ZAMÓWIENIA:

Termin realizacji zamówienia – **do 19.12.2025 r.**

Miejsce realizacji zamówienia/dostawy - Muzeum Sztuki w Łodzi MS1 ul. Więckowskiego 36.

IV. OPIS SPOSOBU PRZYGOTOWANIA OFERTY:

1. Oferta powinna być sporządzona na **formularzu ofertowym** stanowiącym załącznik nr 1 do zapytania.
2. Do oferty należy załączyć:
 - oświadczenie Wykonawcy składane w związku z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. 2025 poz. 514) opatrzone pieczęcią firmową i podpisem osoby upoważnionej - załącznik nr 2 do zapytania.
3. W formularzu ofertowym należy podać ceny jednostkowe netto i brutto za 1 sztukę, wartość netto i brutto oraz sumę wszystkich pozycji netto i brutto.
4. Ofertę należy oznaczyć/w tytule wpisać: **Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi - AG.271.10.2025.Z0.**

V. WARUNKI UDZIAŁU:

Zamawiający nie stawia warunków udziału w postępowaniu.

VI. FORMA, TERMIN I MIEJSCE SKŁADANIA OFERT

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienia dotyczące zapytania ofertowego drogą elektroniczną wyłącznie na stronie internetowej <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl>

2. Oferty należy składać tylko i wyłącznie przez stronę internetową:
a.schiewe@msl.org.pl oraz zamowienia@msl.org.pl w terminie **do dnia 20.11.2025 r. godz. 13:00.**
3. Oferty dostarczone po upływie wskazanego wyżej terminu nie będą rozpatrywane.
4. Zamawiający zastrzega sobie możliwość przedłużenia terminu składania ofert.
5. Termin związania ofertą: 30 dni.
6. Zamawiający nie odpowiada za koszty poniesione przez Wykonawców w związku z przygotowaniem i złożeniem oferty. Wykonawcy zobowiązują się nie podnosić jakichkolwiek roszczeń z tego tytułu względem Zamawiającego.

VII. OCENA OFERT, WYBÓR OFERTY NAJKORZYSTNIEJSZEJ

Wybór najkorzystniejszej oferty nastąpi w oparciu o następujące kryterium: cena 100%.

VIII. INFORMACJA O WYNIKU POSTĘPOWANIA:

O wyniku postępowania Zamawiający poinformuje na stronie internetowej <https://bip.msl.org.pl/>.

IX. POZOSTAŁE INFORMACJE:

1. Zamawiający zastrzega sobie prawo odstąpienia od prowadzonego postępowania, na każdym jego etapie.
2. Informujemy, że złożone w wyniku zapytania oferty mają na celu rozpoznanie rynku i nie mogą stanowić skutecznego roszczenia do zlecenia dostawy lub zawarcia umowy. Niemniej, mogą stać się podstawą do zlecenia stosownej dostawy bądź zawarcia umowy w zakresie realizacji zlecenia lub przekazanie pisemnego Zlecenia dostawy.
3. Zamawiający odrzuci oferty, jeśli ich treść nie będzie odpowiadała treści zapytania.
4. Zamawiający ma prawo wezwać do uzupełnienia i doprecyzowania ofert.
5. Do prowadzonego postępowania nie stosuje się przepisów Ustawy Prawo zamówień publicznych z dnia 11 września 2019 r. (t.j. Dz. U. z 2024 poz. 1320 ze zm.).
6. Zamawiający dopuszcza możliwość negocjacji ceny i innych warunków zamówienia.

X. KLAUZULA RODO:

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, Muzeum Sztuki w Łodzi informuje, że:
 - a) Dane kontaktowe administratora danych: Muzeum Sztuki w Łodzi ul. Więckowskiego 36, 90-734 Łódź, Polska; email: muzeum@msl.org.pl; tel. 42 6338273.
 - b) Dane kontaktowe Inspektora Ochrony Danych Osobowych (IODO): Radosław Rutkowski email: iodo@msl.org.pl.
 - c) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie zapytania o ofertę cenową.
 - d) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2024 poz. 1320), dalej „ustawa Pzp”;

- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy, a w przypadku umów i postępowań o udzielenie zamówienia publicznego, które otrzymały dofinansowanie przez Unię Europejską przez okres wynikający z uchwały w sprawie przyznania dofinansowania oraz obowiązku archiwizacyjnego. \obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
 - w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
 - posiada Pani/Pan:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
 - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
 - nie przysługuje Pani/Panu:
 - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
2. Wykonawca, wypełniając obowiązki informacyjne wynikające z art. 13 lub art. 14 RODO względem osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego w tym postępowaniu składa stosowne oświadczenie zawarte w Formularzu ofertowym.

* **Wyjaśnienie:** skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

** **Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

XI. ZAŁĄCZNIKI

- 1) Załącznik nr 1 – Formularz ofertowy
- 2) Załącznik nr 2 – Oświadczenie Wykonawcy
- 3) Załącznik nr 3 – Opis przedmiotu zamówienia

Andżelika
Bauer

Elektronicznie
podpisany przez
Andżelika Bauer
Data: 2025.11.18
16:14:59 +01'00'

Podpis Kierownika Zamawiającego:

.....

FORMULARZ OFERTOWY

Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi.

AG.271.10.2025.ZO

Nazwa Wykonawcy _____

Adres Wykonawcy _____

TEL.: _____

e-mail: _____

1. Nawiązując do zapytania ofertowego oferujemy wykonanie przedmiotu zamówienia na n/w warunkach:

Przedmiot zamówienia	Producent*	Typ/model*	Rok produkcji*	NR dołączonej karty Produktu oferowanego urządzenia (uwzględniającej konfigurację oferowanego urządzenia)*	Cena netto	Cena brutto
1	3	4	5	6	7	8
Zakup urządzenia firewall typu premium (wraz z wdrożeniem oraz licencjami)						
Zgodnie z Opiszem przedmiotu zamówienia.						

***Należy podać wszystkie do wszystkich urządzeń zaproponowanych w ramach OPZ.**

2. Oświadczamy, że cena ofertowa zawiera wszelkie koszty wykonania zamówienia, zgodnie z warunkami określonymi w zapytaniu ofertowym.
3. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w zapytaniu ofertowym tj. 30 dni

od daty jej otwarcia.

4. Oświadczamy, że w całości i bez zastrzeżeń akceptujemy warunki zawarte w zapytaniu ofertowym i zobowiązujemy się w przypadku wyboru naszej oferty do realizacji zamówienia w miejscu i terminie wyznaczonym przez Zamawiającego.
5. Oświadczam, że wypełniam/em obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

Miejscowość dnia 2025 r.

.....

(pieczęć i podpis osoby uprawnionej do składania
oświadczeń woli w imieniu wykonawcy)

OŚWIADCZENIE WYKONAWCY

Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi.

AG.271.10.2025.ZO

Nazwa Wykonawcy _____
Adres Wykonawcy _____
TEL./FAX: _____
e-mail: _____

składane w związku z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r.

**o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę
oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. 2025 r. poz. 514).**

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.: **Zakup sprzętu informatycznego do zapewnienia bezpieczeństwa systemów i informacji dla Muzeum Sztuki w Łodzi. AG.271.10.2025.ZO** prowadzonego przez Muzeum Sztuki w Łodzi, oświadczam(y), że na dzień składania ofert reprezentowany przeze mnie Wykonawca nie podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. 2025 r. poz. 514).

Oświadczam(y), że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Miejscowość dnia 2025 r.

.....
(pieczęć i podpis osoby uprawnionej do składania
oświadczeń woli w imieniu wykonawcy)

Szczegółowy opis przedmiotu zamówienia

1. UTM z licencjami na okres 36 miesięcy

Nazwa	Wymagania minimalne
Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	- Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. - Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. - Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). - Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. - Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówek pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. - Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. - Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. - Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. - Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. - Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). - System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o

	definiowane przez administratora harmonogramy czasowe.
Intrusion prevention system (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (traffic shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji

	generującej ruch.
Ochrona antywirusowa	1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie. 2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). 3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. 4. Skaner antywirusowy ma pochodzić od europejskiego producenta. 5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 6. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (vpn)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN.

	3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. 3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. 4. Administrator ma mieć możliwość dodawania własnych kategorii URL. 5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 6. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 8. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej

	w oparciu o: - lokalną bazę użytkowników (wewnętrzny LDAP), - zewnętrzną bazę użytkowników (zewnętrzny LDAP), - usługę katalogową Microsoft Active Directory. - Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. - Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: - SSL, - Radius, - Kerberos. - Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. - Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. - Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. - Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). - Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). - Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. - Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
Administracja łączami do internetu (isp)	- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). - Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

	a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.
Administracja urządzeniem	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być

	dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki hasel stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z
--	--

	poziomu interfejsu graficznego.
Raportowanie	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przysyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć zaimplementowane Open API. 10. Urządzenie ma posiadać dwie niezależne partycje np. w celu

	zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
Gwarancja i serwis	1. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie podstawowe ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny. 4. Urządzenie HA ma być objęte serwisem podstawowym na 36 miesięcy.
Parametry sprzętowe	1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. 3. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. 4. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10. 5. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy: a. Moduł z 8 interfejsami miedzianymi 2,5Gbps b. Moduł z 4 interfejsami miedzianymi 10Gbps. c. Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass). d. Moduł z 8 interfejsami miedzianymi 1Gbps. e. Moduł z 8 interfejsami światłowodowymi 1Gbps. f. Moduł z 4 interfejsami światłowodowymi 10Gbps. g. Moduł z 2 interfejsami światłowodowymi 25Gbps. 6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G

	oraz 4G pochodzącego od dowolnego producenta. Wykonawca musi dostarczyć stosowny modem 3G lub 4G oraz uruchomić go zgodnie z konfiguracją wdrażanych urządzeń. Urządzenie musi przejmować pracę połączenia z siecią Internet w przypadku zaniku dostępu do sieci podstawowego łącza Zamawiającego (Zamawiający dostarczy Wykonawcy kartę SIM umożliwiającą dostęp do sieci mobilnej wybranego operatora) 7. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. 8. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. 9. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps. 10. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps. 11. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps. 12. Liczba tuneli VPN IPSec – minimum 1000. 13. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150. 14. Obsługa interfejsów 802.11q (VLAN) – minimum 256. 15. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę. 16. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive. Urządzenie nie ma limitu na liczbę użytkowników. 17. Liczba reguł filtrowania – minimum 16 384. 18. Liczba tras statycznego routingu – minimum 5 120. 19. Liczba tras dynamicznego routingu – minimum 10 000. 20. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 21. Urządzenie musi być wyposażone w moduł TPM.
--	---

2. System logowania i raportowania na okres 36 miesięcy

Nazwa	Wymagania minimalne
Wymagania ogólne:	1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa. 2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V. 3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.

	4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów. 5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP. 6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta. 7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT.
Zarządzanie Logami:	1. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP. 2. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS. 3. Rozwiązanie musi umożliwiać przysyłanie logów do innego serwera logów (funkcja syslog forwarder). 4. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
Rodzaje wyszukiwania	1. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. 2. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.). 3. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne. 4. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP). 5. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów). 6. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
Raportowanie	1. Rozwiązanie musi umożliwiać tworzenie statycznych raportów. 2. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 3. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów. 4. Rozwiązanie musi umożliwiać tworzenie własnych raportów. 5. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.
Zarządzanie incydentami	1. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje

	uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email. 2. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
Wymagania systemowe	1. Liczba zdarzeń na sekundę (EPS): min. 10 000 2. Zarządzanie logami: min 1 rok 3. Liczba obsługiwanych urządzeń min. 500 4. Liczba zapisu zdarzeń na dobę: min 13000 MB 5. System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

3. Szkolenia

W ramach wykonania tego zadania, Zamawiający wymaga od Wykonawcy :

Szkolenie z zakresu administracji urządzeniem UTM – poziom podstawowy – 2 osoby

Zamawiający wymaga dostarczenia vouchera na szkolenie z zakresu obsługi urządzeń UTM proponowanego przez Wykonawcę sprzętu. Voucher musi być ważny przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego instruktora w formie stacjonarnej lub online, w dni robocze. Czas trwania min. trzy dni (minimum 24h). Administrator otrzymuje dostęp do środowiska laboratoryjnego po szkoleniu by lepiej przygotować się do egzaminu producenta. Po szkoleniu wymagane jest otrzymanie zaświadczenia o jego zakończeniu. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

1. Program szkolenia i certyfikacje
2. Przedstawienie firmy UTM i jej produktów
3. Rozpoczęcie pracy z urządzeniem
 - o Rejestracja w strefie klienta i dostęp zasobów
 - o Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
 - o Ustawienia systemowe i uprawnienia administratorów
 - o Instalacja licencji i aktualizacja systemu
 - o Tworzenie kopii zapasowej i przywracanie konfiguracji
4. Zbieranie logów i monitorowanie
 - o Przedstawienie kategorii zbieranych logów
 - o Wykresy historyczne i monitorowanie
5. Obiekty
 - o Typy obiektów oraz ich wykorzystanie
 - o Obiekty sieciowe i obiekt typu „router”
6. Konfiguracja sieci
 - o Tryby pracy urządzenia
 - o Typy interfejsów (Ethernet, modem, bridge, VLAN, GRE/TAP)
 - o Typy routingu oraz ich priorytety
7. Translacja adresów sieciowych (NAT)
8. Translacja połączeń wychodzących (maskarada)
9. Translacja połączeń przychodzących (przekierowanie)
10. Translacja dwukierunkowa (jeden do jeden)
11. Filtrowanie ruchu sieciowego (Firewall)
12. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
 - o Szczegółowy opis parametrów reguły Firewall
 - o Kolejność przetwarzania reguł Firewall i NAT
13. Ochrona aplikacji
 - o Implementacja filtrowania URL dla ruchu http i https
 - o Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
 - o Moduł IPS i stosowanie profili inspekcji
14. Użytkownicy i uwierzytelnianie

15. Konfiguracja usługi katalogowej

- Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
- Rejestracja użytkowników
- Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania

16. Wirtualne sieci prywatne (VPN)

- Koncepty i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
- Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
- Tunele VTI

17. SSL VPN

- Zasada działania
- Konfiguracja

Po zakończonym szkoleniu administrator (wyznaczony pracownika Zamawiającego) ma możliwość przystąpienia do autoryzowanego egzaminu sprawdzającego wiedzę, a po jego zdaniu otrzymania certyfikatu potwierdzającego pomyślne zakończenie egzaminu (Wykonawca ponosi koszty przystąpienia do egzaminu dla 2 wyznaczonych pracowników Zamawiającego, który odbył wcześniej szkolenie ze stosownego zakresu).

Szkolenie z zakresu administracji urządzeniem UTM – poziom ekspercki – 1 osoba.

Zamawiający wymaga dostarczenia vouchera na szkolenie z zakresu obsługi urządzeń UTM proponowanego przez Wykonawcę sprzętu na poziomie eksperckim. Voucher musi być ważny przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego instruktora w formie stacjonarnej lub online, w dni robocze. Czas trwania min. trzy dni (minimum 24h). Administrator otrzymuje dostęp do środowiska laboratoryjnego po szkoleniu lepiej przygotować się do egzaminu producenta. Po szkoleniu wymagane jest otrzymanie zaświadczenia o jego zakończeniu. Zamawiający dopuszcza typ szkolenia, do którego Administrator może podejść dopiero po pomyślnym zdaniu certyfikacji na poziomie podstawowym. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

1. Szczegółowe omówienie działania modułu IPS

- Różnice pomiędzy IPS a IDS
- moduł IPS
- Różne tryby analizy
- Profile oparte na protokołach i aplikacjach

2. Infrastruktura klucza publicznego

- Podstawy szyfrowania symetrycznego - i asymetrycznego
- Typy szyfrowania
- Infrastruktura klucza publicznego w rozwiązaniach UTM
- Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników

3. SSL Proxy

- Zasada działania
- Konfiguracja SSL Proxy
- Zaawansowana konfiguracja tuneli IPSec VPN
- Szczegółowy opis działania mechanizmu NAT traversal
- Obsługa funkcji DPD (Dead Peer Detection)

- Architektura sieci VPN typu „gwiazda” i „mesh”
 - NAT w sieciach IPSec VPN
 - Konfiguracja zapasowego - tunelu IPSec VPN
 - Konfiguracja tuneli Site-to-Site w oparciu - certyfikaty
 - Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site)
4. GRE i GRE-TAP
- Zasada działania
 - Konfiguracja i instalacja
5. Transparentne uwierzytelnianie użytkowników
- Zasada działania
 - Metoda uwierzytelniania SPNEGO
 - Metoda uwierzytelniania oparta na certyfikatach SSL
6. Wysoka dostępność (HA)
- Zasada działania
 - Kreator umożliwiający tworzenie i konfigurowanie klastra HA
 - Konfiguracja interfejsu sieciowego
 - Zaawansowana konfiguracja

Po zakończonym szkoleniu administrator (wyznaczony pracownika Zamawiającego) ma możliwość przystąpienia do autoryzowanego egzaminu sprawdzającego wiedzę, a po jego zdaniu otrzymaniu certyfikatu potwierdzającego pomyślne zakończenie egzaminu. (Wykonawca ponosi koszty 2 przystąpienia do egzaminu wyznaczonego pracownika Zamawiającego, który odbył wcześniej szkolenie ze stosownego zakresu).

4. Wdrożenie urządzeń UTM

W ramach wykonania tego zadania, Zamawiający wymaga od Wykonawcy wstępnej konfiguracji oraz wdrożenia oferowanego urządzenia UTM zgodnie z wymaganiami Zamawiającego. W skład konfiguracji będzie wchodzić:

1. Przygotowanie i analiza przedwdrożeniowa
 - Zebranie wymagań i przeprowadzenie analizy obecnej infrastruktury sieciowej Zamawiającego.
 - Inwentaryzacja istniejącej adresacji IP, VLAN, reguł firewall, VPN, NAT, tras statycznych i dynamicznych.
 - Weryfikacja istniejących urządzeń brzegowych oraz topologii.
 - Opracowanie projektu logicznego konfiguracji UTM, obejmującego segmentację sieci, strefy bezpieczeństwa, polityki dostępu, integracje i mechanizmy HA (jeśli dotyczy).
2. Konfiguracja podstawowa
 - Konfiguracja adresacji interfejsów, stref bezpieczeństwa, routingu statycznego i/lub dynamicznego.
 - Konfiguracja VLAN i przypisanie ich do odpowiednich portów.
 - Konfiguracja NAT i polityk przekierowań.
 - Integracja z NTP, DNS, syslogiem i serwerem czasu.
 - Utworzenie kont administratorów zgodnie z polityką bezpieczeństwa.
 - Segmentacja sieci oraz wdrożenie polityk bezpieczeństwa
 - Kategoryzacja treści WWW

3. Konfiguracja VPN
 - o Konfiguracja VPN dla użytkowników
 - o Konfiguracja MFA dla użytkowników oraz administratorów
4. High Availability (HA)
 - o Konfiguracja klastra HA
 - o Synchronizacja konfiguracji między urządzeniami
 - o Test przełączenia
5. Testy bezpieczeństwa i odbiorcze
 - o Test działania wszystkich polityk i modułów bezpieczeństwa
 - o Testy VPN, routingu, segmentacji, NAT, failover
 - o Weryfikacja poprawności konfiguracji
6. Dokumentacja powdrożeniowa
 - o Topologia sieci po wdrożeniu.
 - o Zestawienie wszystkich polityk firewall.
 - o Lista VLAN i stref bezpieczeństwa.
 - o Konfiguracja VPN.
 - o Instrukcja zarządzania i tworzenia nowych polityk.
 - o Dane dostępne dla administratorów.

5. Wsparcie 24H w zakresie UTM

Wykonawca zapewni Zamawiającemu **całodobowe wsparcie techniczne (24/7/365)** w zakresie konfiguracji, działania oraz bezpieczeństwa urządzenia UTM przez okres **12 miesięcy od dnia podpisania protokołu odbioru wdrożenia**.

Wsparcie obejmuje w szczególności:

1. **Możliwość zgłaszania incydentów, awarii, problemów konfiguracyjnych lub konieczności wprowadzenia zmian** w konfiguracji UTM **o dowolnej porze**, tj. 24 godziny na dobę, 7 dni w tygodniu.
2. **Zdalną reakcję Wykonawcy**, polegającą na:
 - o diagnostyce zgłoszonego problemu,
 - o wprowadzeniu niezbędnych zmian konfiguracyjnych,
 - o przywróceniu prawidłowego działania usług,
 - o konsultacji technicznej dotyczącej funkcjonowania UTM.
3. Wsparcie obejmuje także:
 - o doprecyzowanie lub aktualizację reguł firewall,
 - o modyfikację polityk bezpieczeństwa,
 - o korekty konfiguracji VPN,
 - o analizę alertów bezpieczeństwa i logów,
 - o pomoc w przypadku wykrycia zdarzeń mogących świadczyć o incydencie bezpieczeństwa.
4. Wsparcie świadczone będzie **zdalnie** poprzez e-mail, telefon lub bezpieczne połączenie zdalne. W uzasadnionych przypadkach dopuszcza się wsparcie onsite
5. Wsparcie nie obejmuje zmian wykraczających poza zakres wdrożonej konfiguracji lub rozbudowy urządzenia o nowe moduły; wszelkie prace dodatkowe będą ustalane odrębnie.

Uwaga:

Wszystkie elementy niewymienione szczegółowo, a niezbędne do wdrożenia i montażu systemu (kable, uchwyty, śruby montażowe i inne), Wykonawca zobowiązany jest dostarczyć.

Zapewnienie tych elementów stanowi integralną część oferty i nie może być traktowane jako koszt dodatkowy.
